A Comprehensive Survey on DDoS Attacks on various Intelligent Systems and It's Defense Techniques

Akshat Gaurav

***Abstract*—In recent times, due to the endemic COVID-19, the use of the online service has increased. The most important requirement of these on-line services is that they have to provide their service efficiently and continuously. But the availability and efficiency of the online source are affected by the DDoS attack, which the attacker uses, and the attacker uses to attack the availability and computation power of online sources. A DDoS attack is a reliable tool for cyber-attackers because there is no efficient method which can detect or filter it properly. In this paper, we give a detailed analysis of DDoS attack architecture and different defense techniques.**

***Index Terms*—DDoS, Volumetric DDoS attack, Resource depletion attack, DDoS attack tools.**

I. Introduction

In the last decade, there has been a rapid development of technologies that can fulfill day-to-day human requirements like online bill payments, online shopping, etc., and also control and monitor the key systems that are important in human development like water management, power production and distribution, gas, etc., also known as Critical Infrastructure (CI). These technologies use cloud computing [1], [2], smart devices [3], big data [4], IoT [5], and the Internet as their communication medium, so if there is a malfunctioning on the Internet, then it will affect human life directly or indirectly.

Due to this dependency of human life on the Internet, attackers target the Internet to affect human life [6]–[9]. One of the most popular methods of doing this is through a DDoS attack, which generates large fake traffic that can disrupt the normal working of the Internet. DDoS attacks [10]–[13] architecture is presented in Fig. 1. Therefore, legitimate users are not able to connect to the services they want to connect to [14], [15], [15]–[17]. But sometimes services on the Internet are also disturbed by the large amount of traffic generated by legitimate users. This leads to the scenario called the Flash Crowd (FC) attack [18]. In DDoS [19]–[21] and FC a large amount of traffic is generated, but in the former case the generated traffic is by malicious users, but in the latter case it is by legitimated users, which is important to the victim. Therefore, the main objective of this thesis is to detect DDoS attack traffic accurately and efficiently and also differentiate DDoS traffic [22] from FC traffic [23], [24].

A. Different Phases of DDoS Attack

The three phases of DDoS attacks are as follows:

Akshat Gaurav, Ronin Institute, Montclair, New Jersey 07043, U.S., (e-mail: akshat.gaurav@ronininstitute.org)

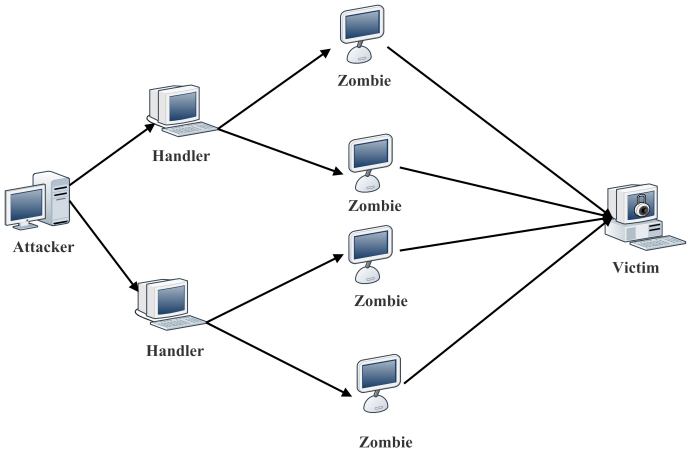

Fig. 1: DDoS Attack Architecture

- Target Selection - This is the most elementary phase of the DDoS attack; in this phase, attacker selects its target. The selection of a target by the attacker represents the intention or motive of the attacker. The motive may be of the following:
  - Revenge - Sometimes the reason behind the target selection is of personal rivalry. There are many cases where an attacker conducts a DDoS attack on the victim to take his personal revenge.
  - Fame - Sometimes the attacker selects the target to get fame. In some cases the attacker thinks that if he is able to crash some well-known or big-brand company server, then he gets fame in the hacker community.
  - Cyber Warfare - Sometimes the attack target is not to crash a single server but to crash the grout of servers which indirectly affect the working of entire government, i.e. attacks on Estonia and Georgia [25]
  - Intellectual Challenge - Some attackers conduct DDoS attack only to test their abilities or in order to learn some new technology.
  - Material gain - Sometimes DDoS attacks are conducted by different companies against their rival companies to damage their reputation and resources.
- Agent Recruitment - After selecting the target, the attacker starts increasing the number of zombie or compromised computers from which real attack starts. There are mainly two methods by which the attacker selects the

compromised computers.

  - Active method - In this method, the attacker scans-method an the network with the help of some scanning tool like Nmap [26] in order to find the systems that have known vulnerabilities. After getting the list of vulnerabilities of a system, the attacker uses that vulnerability to access the system. There is a number of organizations, such as Common Vulnerabilities and Exposures (CVE)(Common Vulnerabilities and Exposures) organization, which discloses all the vulnerabilities of different systems from time to time. After getting access to the system, the attacker installed malicious software in it so that the system can act like a zombie machine. Some of the malicious software which is used by attackers are Trojan horse [27] and buffer over flow [28].
  - Passive Method - In this method attacker utilizes the vulnerabilities of a web browser on the victim's system; for this, either an attacker shares malicious files or built fake websites.
- Actual attack - In this phase, the attacker ordered the compromised system to attack the target system. The type of attack depends on the type of victim as represented in Table I.

TABLE I: Different types of Attack

Target	Possible Attack	Impact
Server(Web, Mail, Proxy)	Malformed packet attack, Flooding attack	Unavailability of system resources, System run out of memory
Server(Storage)	Flooding attack	Server Crash
Communication Bandwidth	Flooding attack	Bandwidth Depletion

II. DDoS Attack Types

In DDoS attack, the attacker attacks the availability of the victim's system. To make the victim unavailable to legitimated users, an attacker may flood its bandwidth with unwanted packets or attacks on the available resources of the victim [29]–[31]. According to these methods, DDoS attacks are classified into two groups, one is bandwidth attacks and the other is resource depletion attacks; Fig. 2 explains this basic attack classification.

A. Bandwidth Attack

In this type of attack scenario, attacker uses compromised systems i.e., Bot/Zombies [32] to generate large amount of traffic which consumes victim's bandwidth or reduce its computation power due to which victim's ability to serve the legitimated users decreases. This attack type is further divided into flood attack and amplification attack.

1) Flood Attack: There are three common types of flood attacks, UDP (User Datagram Protocol) flooding, HTTP (Hyper Text Transfer Protocol) flooding, and ICMP (Internet Control Message Protocol) flooding [33].

- **UDP Flooding Attack** - In this type of attack, the attacker sends a large amounts of UDP packets to random ports on the victim's system. Victim's machine processes the incoming UDP packets, and if no application is running on the specific port, then it sends back an ICMP packet to show that the destination is unreachable. But this consumes the victim's resources. So this type of attack consumes the resources of the victim's system.
- **HTTP Flooding Attack** - In this form of attack, the attacker sends large amount of HTTP requests, in the form of POST of GET requests, threw legitimate TCP connection. Processing of these fake requests consumes the resources of victim's machine.
- **ICMP Flooding Attack** - ICMP packets are designed to manage the network. One of the uses of ICMP packets is to check the reachability of the destination system by sending ICMP_ECHO_REPLY packets. If any system receives ICMP_ECHO_REPLY then it sends ICMP packet to the source of that packet. However, the attacker utilized this property of the protocol. So in this attack, an attacker sends a large number of ICMP_ECHO_REPLY packets with spoofed source address, which in turn consumes the resources of the victim's machine.

2) Amplification Attack: In this type of attack, the attacker in the scenario uses the ICMP protocol to flood the bandwidth of the victim. Attacker broadcasts the ICMP-ECHO in the network with the source address of packets spoofed as the victim's IP address, so all the systems in the network reply this echo request, and this generates a large amount of traffic which crashes the victim's system. This type of attack is often called the Smurf attack [34] and Fig. 3 explains this more clearly.

B. Resource Depletion Attack

In Resource depletion attack attacker either misuses the network protocols or sends malformed packets on the victim's machine, which in turn consumes the victim's resources, and it is not available for legitimated users. Different types of resource depletion attacks are explained below.

1) Protocol Exploitation Attack:

- **TCP-SYN Attack** - In this type of attack, the attacker exploits standard protocols such as the TCP (Transmission Control Protocol) three-way handshake protocol [35]. Real communication begins after the three-way handshake that occurs in the TCP protocol between the source and destination. SYN packet (synchronization packet) is initially sent from the source to the destination. The destination receives it and stores it in a queue before sending ACK + SYN packet, which is an acknowledgment of the received SYN packet as well as the source address's SYN packet. The source sends an ACK (acknowledgment) to the destination after receiving an ACK+SYN packet from the destination, and the destination removes the source

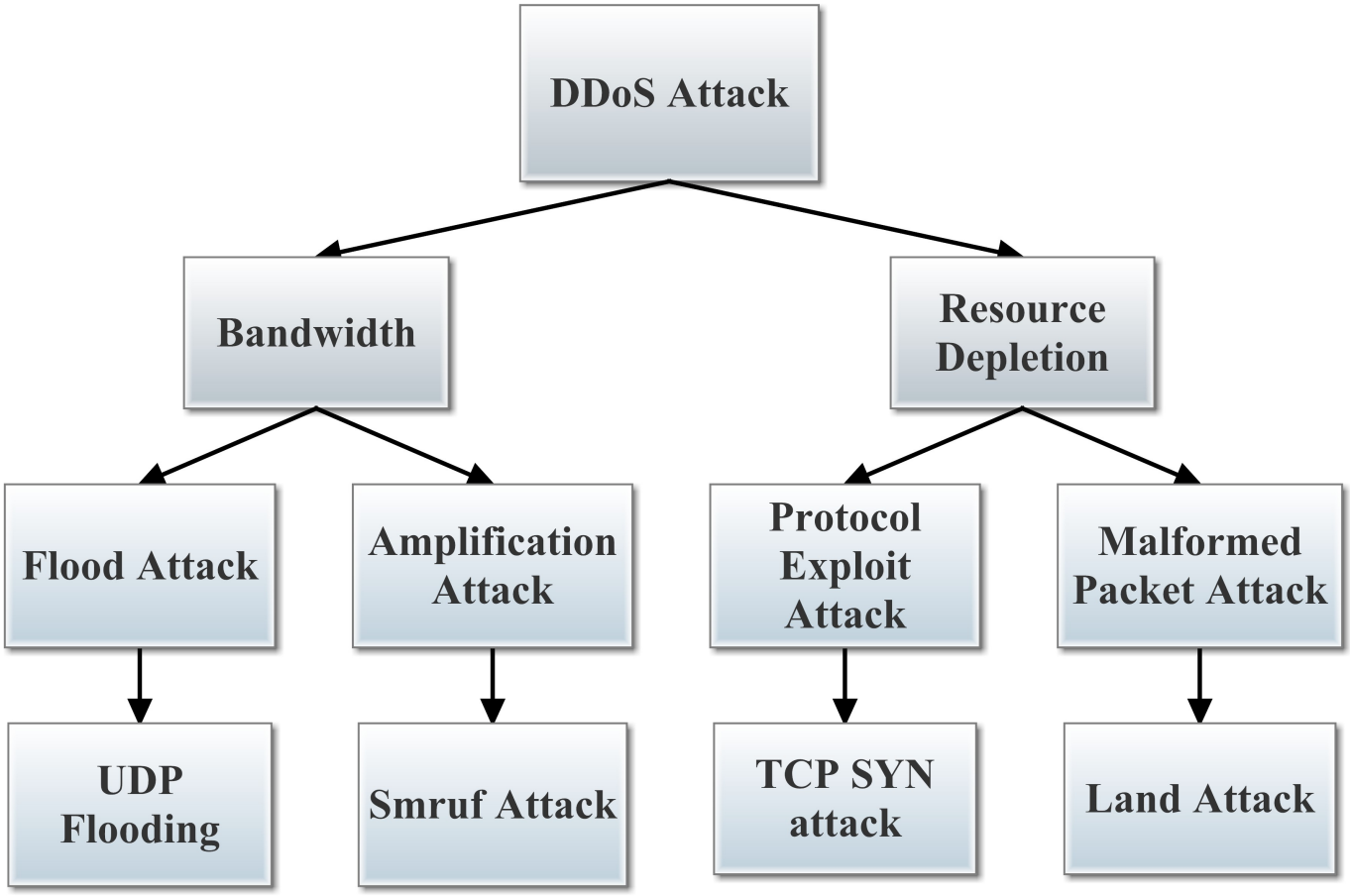

Fig. 2: DDoS Attack Classification

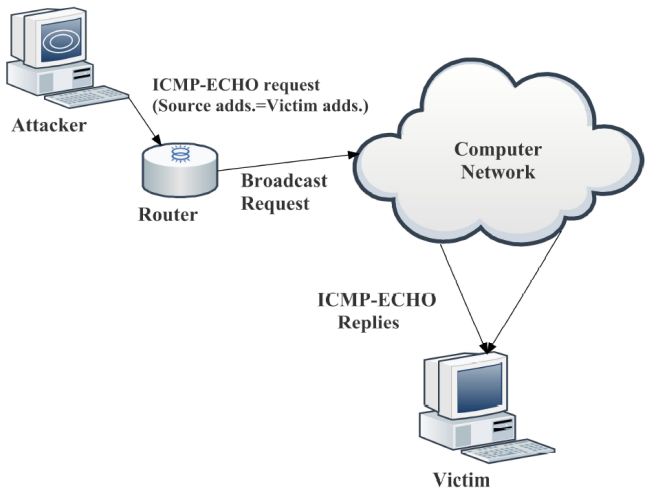

Fig. 3: Smruf Attack

address from its queue. SYN packets are sent in huge quantities in TCP-SYN attacks by the attacker, causing a backlog for genuine users and making it impossible for them to get service. Fig. 4 represents this scenario.

– **PUSH+ACK attack** - In TCP communication, first the packets are stored in a buffer and when the buffer is full all the packets are sent to the destination. But if receiver sets the PUSH bit set in TCP header then sender transmits all the packets before the overflow of TCP buffer. So in this type of attack, attacker sends a large number of ACK bits with PUSH bit set. The victim then emptys all the packets in the TCP buffer and sends the acknowledgment to the source. Therefore due to this type of attack, the victim is unable to process a large amount of data and hence its processing capabilities are reduced.

2) Malformed Packet Attack:

– **Ping of Death** [36] - In this attack attacker sends oversized ICMP packets. The normal size of an ICMP packet is 64 bytes, so attacker send packet of larger length, this will overburden the victim and its resources get depleted.
– **Teardrop Attack** [37] - In this form of attack attacker exploits the TCP/IP fragment vulnerability. So, attacker sends many overlapping fragments. Thus, all the resources at the victim end get consumers to arrange these fragments, and it is not available for legitimate users.
– **Land Attack** - In this attack format, the attacker sends packets with the same source and destination address as represented in Fig. 5. This again overburdens the victim's system and exhausts its resources.

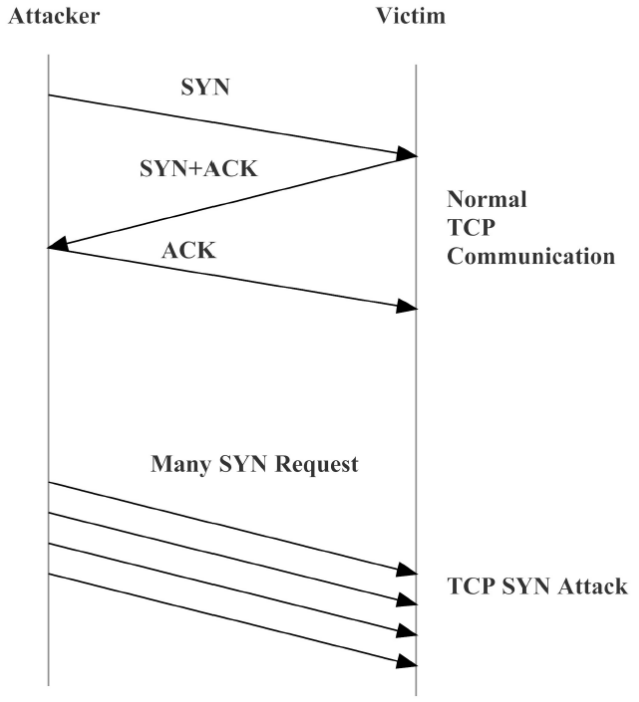

Fig. 4: TCP-SYN Attack

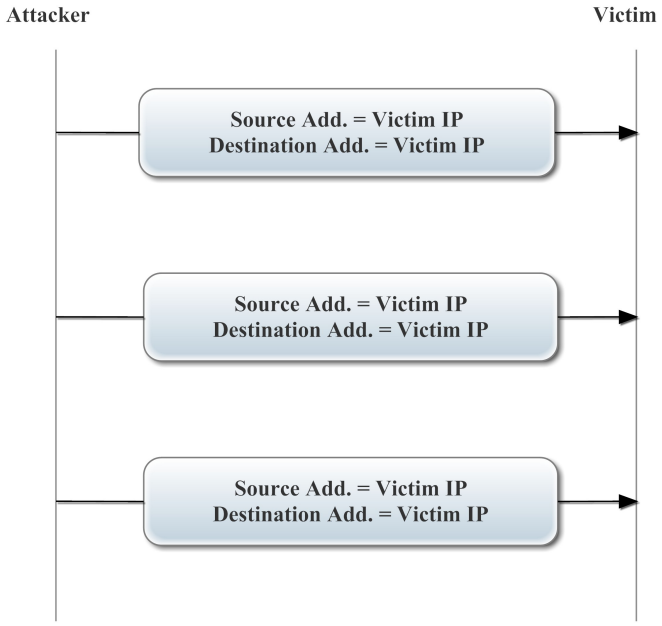
Attacker
Victim
Source Add. = Victim IP
Destination Add. = Victim IP
Source Add. = Victim IP
Destination Add. = Victim IP
Source Add. = Victim IP
Destination Add. = Victim IP

Fig. 5: Malformed Packet Attack

III. Tools

There are many tools by which anyone can start the DDoS attack [38] [39]. Some important tools are represented below.

- Trin00 - This is the first DDoS attack tool used by attackers [40]. This tool uses UDP packets to flood the victim's bandwidth. The attacker installs Trin00 on those systems that suffer from buffer overrun exploitation. Another feature of Trin00 is that in this TCP packets are used as a communication medium between attackers and handlers, and UDP packets are used as a communication medium between handlers and bots [41], [42]. All communication between handlers and bots is encrypted by symmetric key encryption, so it is difficult for anyone to decode the instructions.
- Tribe Flood Attack [TFN] - It was written in 1999 [43]. It is a command-line operating tool. It can perform bandwidth depletion attack and resource exploitation attack. It can also perform UDP flood attack, TCP-SYN attack, ICMP flood attack, and Smurf attack. In this tool, handlers and bots communicate by ICMP_ECHO_REPLY packets. It uses no encryption for communication and mostly affects a system that uses Solaris 2.x and Red Hat Linux 6.0 operating systems.
- TFN2K (Tribel Flood Network 2000) - It is the same as that of the TFN tool [44]. The only difference is that it uses an encryption method for communication between the attacker and bots. The communication is done by UDP, TCP, or ICMP packets.
- Stacheldraht - It is based on the TFN tool [45]. Moreover, it uses symmetric key encryption between handlers and bots. In this, bots are automatically updated when they connected to the Internet and it uses telnet connection for communication between handlers and bots.
- Mstream- It generates many TCP-ACK packets that flood the victim's bandwidth [46]. It uses TCP or UDP for communication between handlers and bots with no encryption involved during the communication.
- Trinity v3 - It can generate TCP fragmentation flood, TCP RST packet floods, TCP random flag packet flood and TCP established flood in addition to UDP, TCP-SYN, TCP NULL packet flood attacks [47]. It can generate spoofed IP packets, making it harder to detect the source of the attack.
- Knight- The first use of this tool was in 2001 [47]. It can work on a Windows-based operating system. It uses TCP SYN packets or UDP packets to flood the victim's system.
- Low orbit ion Cannon (LOIC) - It was created and used by the hacker group Anonymous [48]. It can perform TCP, UDP, HTTP flooding attacks.
- High Orbit Ion Cannon (HOIC)- It is the latest version of LOIC. It can only perform the HTTP flooding attack. It also randomizes the request, so each packet goes to a random port and the spoofed source address is also random. Hence, it is difficult for any IDS (Intrusion Detection System) to filter out the attack packets.

The label II represents the series of attack tools that attackers frequently use. The property of each tool is different, but the basic aim of each tool is to flood the victim's system or network.

IV. DDoS Attack Detection

Previous section defines different DDoS attack techniques and different attack tools which are generally used by attackers to initiate a DDoS attack. However, there are also many DDoS

TABLE II: Summery of DDoS Attack Tools

DDoS attack tool	Types of flooding	Communication Method	Encryption
Trin00	UDP	Attacker to handler TCP Handker to bot UDP Bot to handler UDP	NO
TFN	ICMP, UDP, TCP	Attacker to handler third party program Handler to bot ICMP Bot to handler none	NO
TFN2K	ICMP, UDP, TCP, Mixed	Attacker to handler none Handler to bot mixture of ICMP, TCP, UDP Bot to handler none	Yes
Stacheldraht	ICMP, UDP, TCP	Attacker to handler TCP Handler to bot ICMP and TCP Bot to handler none	Yes
Shaft	ICMP, UDP, TCP, Mixed	Attacker to handler TCP Handler to bot UDP Bot to handler none	No
Mstream	TCP	Attacker to handle TCP Handler to bot UDP Bot to handler UDP	No
Knight	UDP, TCP	Use IRC for communication	No
Trinity	TCP, UDP	Use IRC for communication	No

defense techniques [49]–[51] that can detect different DDoS attacks [52]–[55], such as AI [56]–[58], cryptography [59], machine learning [60], [61]. DDoS defense techniques are broadly differentiated into three groups [62].

- Attack Prevention techniques .
- Attack traceback techniques
- Attack filtering techniques.

Classification of defence techniques is represented in Fig. 6.

A. Attack Prevention

- Load blanching - It is a technique that is adopted by ISPs. In this technique, ISP provides some additional bandwidth to the victim at the time of DDoS attack, so it can serve its legitimated users. Sometime ISP also shift the extra load of one server to other servers to save the servers from crash.
- Throttling - This is a new proposed method to protect systems from flooding attacks [63]. In this technique, each router decides some upper limit to its outgoing traffic and if incoming traffic is more than the upper limit then router will filter the extra traffic. But the main limitation of this type of technique is that routers are not able to differentiate malicious traffic from legitimate traffic.
- Honeypots - These are the systems with limited security and are therefore used to attract attackers [64]. These systems are used to gain information about the attacker by storing all the information about the attacker in its log files. So these systems are places along with the systems to be protected and periodicity monitored. If attacker attacks these systems, then he can easily be identified.
- Firewalls - It will save the system from simple flooding attacks [65]. The firewall sets simple rules and filters packets according to those rules. But the main limitation of a firewall is that it is unable to differentiate malicious traffic from legitimate traffic.
- IP Hopping - In this process, the IP address of the victim system is periodically changing, and a new IP address is selected from the predefined pool of IP addresses [66]. Once the new IP address is set for the system, this information is passed to all routers on the network. Thus, the router passes the incoming packets to a new IP address. But this technique is also not a full proof technique against DDoS attacks as attackers can easily find the new address and divert the attack traffic towards that IP address.
- SOS - It is a basic architecture used to protect the victim system from DoS attacks [67]. In this method, the system who wants to send packets first gets verified by secure overlay node access point (SOAP). After verification, the source sends the packets to the SOAP and then the SOAP forwards these packets to some beacon node, which again forwards the packet to an anonymous secret node. The location of the secret node is known to the limited beacon nodes. Therefore, according to the security threat, different numbers of secret nodes are placed around the victim's system. As traffic can only reach the victim, they threw these secret nodes, but their locations are not known to the attacker. Therefore, this architecture provides a good defense against DOS and DDoS attacks.

B. Attack Trace back

- Probabilistic Packet Marking - In this scheme, the unused fields in IP header, e.g. fragment offset, option, padding, etc., are used for marking the packets and storing the route information. In this scheme, in IP header five information are saved (a) initial router address, (b) final router address, (c) flag, (d) distance, and (e) mark. When ever a packet comes to the router, it marks the packet

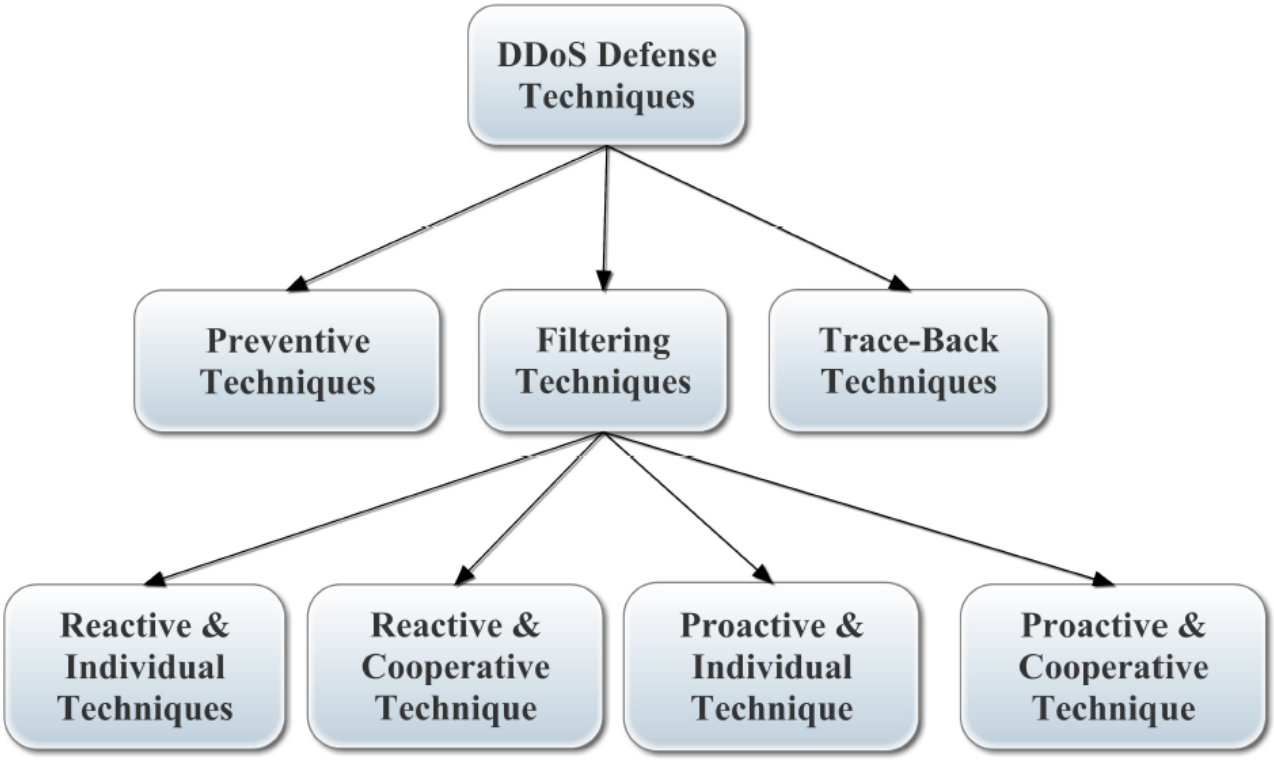

Fig. 6: Different defense Techniques against DDoS attack

with a set probability (1/20000) and also adds its address on the IP header. When a packet passes through the next router, it also adds its address toto the IP header, increases the distance field by one, and sets the flag. Now, all preceding routers only increment the distance field. By this packet marking technique, the router address near the source of is detected, this technique is represented in Fig. 7. In Fig. 7 router R1 first adds its address in the IP header and increments the distance field, and then router R2 also adds its address in the IP header and sets the flag bit. Then all subsequent routers only increment the distance field in the IP header. Therefore, by this technique, it is easy to find the router address near the source.

- Log Information - Log information is also useful for tracing the attacker. By analyzing the log information stored in the honeypot, the firewall and IPS/IDS network administrator can track the source of the attacker.

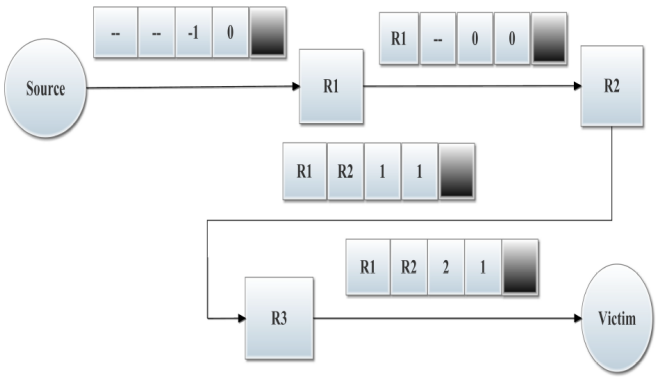

Fig. 7: Probabilistic Packet Marking Technique

C. Attack Filtering

the attack filtering process can be divided into four groups, which are explained below.

1) Reactive & Individual: In this case, each filter stays active for the entire attack period only, and stores information about incoming packets locally. In this type of filtering, there is no exchange of information between two routers. The hopcount filter [68] is an example of this type of filter. This filtering method uses the TTL (time to live) time to field in the IP packet header to differentiate spoofed packets from legitimate packets. In general communication, as the packet moves through different routers, its TTL value decreases. Each router maintains a table known as IP2HC (IP To Hopcount) table which contains source IP address and its matching TTL value at that router, so during the attack the router compares the IP address of the input packet and its TTL value with the stored value, if the value is correct then only it allows the packet to pass, otherwise the packet is filtered out. This scenario is represented in Fig. 8, if a normal packet takes two hops to reach from system 1 to system 2 threw router 1 and router 2. But if any of the in-between routers, i.e. router 1 or

router 2 get a wrong hop count of the incoming packet from system 1 then it will simply discard that packet.

2) Reactive & Cooperative: In this type of filtering, each filter remains active only during the attack and stores information about incoming packets locally. It stores only information from the attack period. In this type of filtering exchange of information related to packet filtering takes place between two routers.

3) Proactive & Individual: In this type of filtering, each filter stays active all the time and stores information from incoming packets locally, so each filter remains active all the time. In this type of filtering, there is no exchange of information between two routers. Ingress / exit filtering [69] is a good example of this type of filtering. In this method, packets are scanned when they enter or leave the computer network. If the packets did not meet certain criteria, they are blocked. Ingress filtering means scanning of incoming packets, and exit filtering means scanning outgoing packets. This technique is represented in Fig. 9

4) Proactive & Cooperative: In this type of filtering, each filter remains active all the time and stores information about incoming packets locally. In this type of filtering, exchange of information between two routers takes place. Thus, it starts filtering the attack traffic at an earlier stage of attack; ScoreForCore [70] is an example of this type of filtering technique.

V. Conclusion

In DDoS attack, a large number of compromised systems from different geographical location generate a large amount of traffic to attack victim's system, which in turn crash the system or reduce its computational power. Therefore, efficiently and accurately detecting DDoS attacks is always a key research challenge. In this context, we discuss DDoS attacks and defense techniques in this paper. This paper will help future researchers and scholars to understand the DDoS attack more closely.

References

[1] A. M. Manasrah, A. Aldomi, and B. B. Gupta, "An optimized service broker routing policy based on differential evolution algorithm in fog/cloud environment," *Cluster Computing*, vol. 22, no. 1, pp. 1639–1653, 2019.

[2] C. L. Stergiou, K. E. Psannis, and B. B. Gupta, "Infemo: flexible big data management through a federated cloud system," *ACM Transactions on Internet Technology (TOIT)*, vol. 22, no. 2, pp. 1–22, 2021.

[3] A. Gaurav and A. K. Singh, "Light weight approach for secure backbone construction for manets," *Journal of King Saud University-Computer and Information Sciences*, vol. 33, no. 7, pp. 908–919, 2021.

[4] R. C. Joshi and B. B. Gupta, *Security, Privacy, and Forensics Issues in Big Data*. IGI Global, 2019.

[5] B. B. Gupta, A. Gaurav, K. T. Chui, and C.-H. Hsu, "Identity-based authentication technique for iot devices," in *2022 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2022, pp. 1–4.

[6] S. Gupta and B. B. Gupta, "Php-sensor: a prototype method to discover workflow violation and xss vulnerabilities in php web applications," in *Proceedings of the 12th ACM International Conference on Computing Frontiers*, 2015, pp. 1–8.

[7] G. N. Nguyen, N. H. Le Viet, M. Elhoseny, K. Shankar, B. Gupta, and A. A. Abd El-Latif, "Secure blockchain enabled cyber–physical systems in healthcare using deep belief network with resnet model," *Journal of Parallel and Distributed Computing*, vol. 153, pp. 150–160, 2021.

[8] M. Xu, J. Peng, B. Gupta, J. Kang, Z. Xiong, Z. Li, and A. A. Abd El-Latif, "Multi-agent federated reinforcement learning for secure incentive mechanism in intelligent cyber-physical systems," *IEEE Internet of Things Journal*, 2021.

[9] R. Kumar and B. Gupta, "Stepping stone detection techniques: Classification and state-of-the-art," in *Proceedings of the international conference on recent cognizance in wireless communication & image processing*. Springer, 2016, pp. 523–533.

[10] J. Mirkovic and P. Reiher, "A taxonomy of ddos attack and ddos defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39–53, 2004.

[11] P. Negi, A. Mishra, and B. B. Gupta, "Enhanced cbf packet filtering method to detect ddos attack in cloud computing environment," *arXiv preprint arXiv:1304.7073*, 2013.

[12] B. B. Gupta, M. Misra, and R. C. Joshi, "An isp level solution to combat ddos attacks using combined statistical based approach," *arXiv preprint arXiv:1203.2400*, 2012.

[13] A. Mishra, B. B. Gupta, and R. C. Joshi, "A comparative study of distributed denial of service attacks, intrusion tolerance and mitigation techniques," in *2011 European Intelligence and Security Informatics Conference*. IEEE, 2011, pp. 286–289.

[14] Z. Zhou, A. Gaurav, B. Gupta, H. Hamdi, and N. Nedjah, "A statistical approach to secure health care services from ddos attacks during covid-19 pandemic," *Neural Computing and Applications*, pp. 1–14, 2021.

[15] A. Gaurav, B. Gupta, C.-H. Hsu, D. Peraković, and F. J. G. PEÑALVO, "Filtering of distributed denial of services (ddos) attacks in cloud computing environment," in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2021, pp. 1–6.

[16] P. Gulihar and B. B. Gupta, "Cooperative mechanisms for defending distributed denial of service (ddos) attacks," in *Handbook of Computer Networks and Cyber Security*. Springer, 2020, pp. 421–443.

[17] A. Gaurav, B. Gupta, F. J. G. Peñalvo, N. Nedjah, and K. Psannis, "Ddos attack detection in vehicular ad-hoc network (vanet) for 5g networks," in *Security and Privacy Preserving for IoT and 5G Networks*. Springer, 2022, pp. 263–278.

[18] A. Gaurav and A. K. Singh, "Entropy-score: A method to detect ddos attack and flash crowd," in *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*. IEEE, 2017, pp. 1427–1431.

[19] B. Gupta, A. Gaurav, and D. Peraković, "A big data and deep learning based approach for ddos detection in cloud computing environment," in *2021 IEEE 10th Global Conference on Consumer Electronics (GCCE)*. IEEE, 2021, pp. 287–290.

[20] A. Gaurav, B. B. Gupta, and P. K. Panigrahi, "A novel approach for ddos attacks detection in covid-19 scenario for small entrepreneurs," *Technological Forecasting and Social Change*, vol. 177, p. 121554, 2022.

[21] A. Dahiya and B. Gupta, "A pbnm and economic incentive-based defensive mechanism against ddos attacks," *Enterprise Information Systems*, vol. 16, no. 3, pp. 406–426, 2022.

[22] B. B. Gupta and A. Dahiya, *Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges and Countermeasures*. CRC press, 2021.

[23] B. B. Gupta, A. Dahiya, C. Upneja, A. Garg, and R. Choudhary, "A comprehensive survey on ddos attacks and recent defense mechanisms," *Handbook of Research on Intrusion Detection Systems*, pp. 186–218, 2020.

[24] A. Mishra, N. Gupta, and B. Gupta, "Defense mechanisms against ddos attack based on entropy in sdn-cloud using pox controller," *Telecommunication systems*, vol. 77, no. 1, pp. 47–62, 2021.

[25] R. Stapleton-Gray and W. Woodcock, "National internet defense—small states on the skirmish line," *Communications of the ACM*, vol. 54, no. 3, pp. 50–55, 2011.

[26] G. F. Lyon, *Nmap network scanning: The official Nmap project guide to network discovery and security scanning*. Insecure, 2009.

[27] R. W. Butler, "Alternative tourism: Pious hope or trojan horse?" *Journal of Travel Research*, vol. 28, no. 3, pp. 40–45, 1990.

[28] C. Cowan, F. Wagle, C. Pu, S. Beattie, and J. Walpole, "Buffer overflows: Attacks and defenses for the vulnerability of the decade," in *DARPA Information Survivability Conference and Exposition, 2000. DISCEX'00. Proceedings*, vol. 2. IEEE, 2000, pp. 119–129.

[29] A. Dahiya and B. Gupta, *How IoT is Making DDoS Attacks More Dangerous*. insights2techinfo.com, 2021. [Online]. Available: https://insights2techinfo.com/how-iot-is-making-ddos-attacks-more-dangerous/

[30] D. Singh, *Captcha Improvement: Security from DDoS Attack*. Insights2Techinfo, 2021.

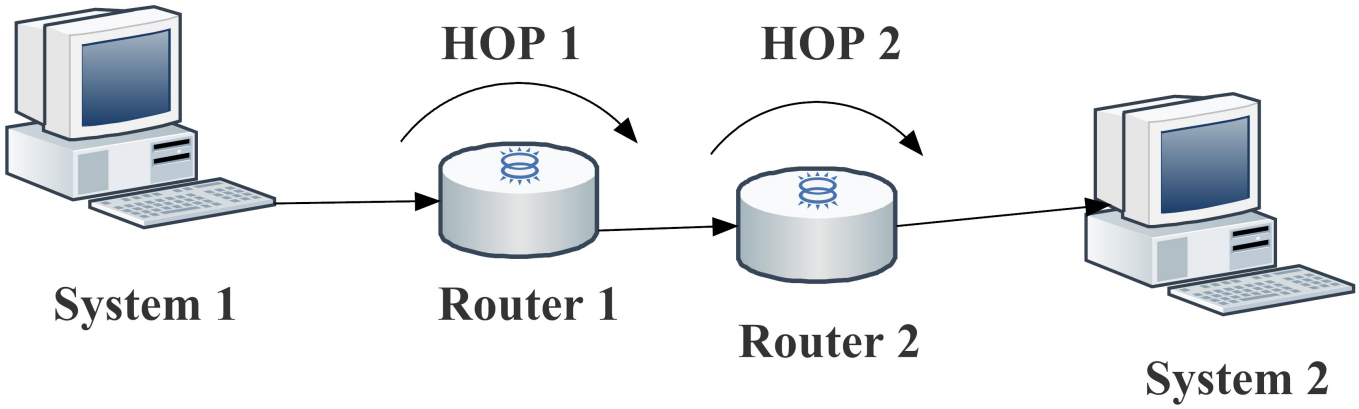

Fig. 8: Hopcount Filtering

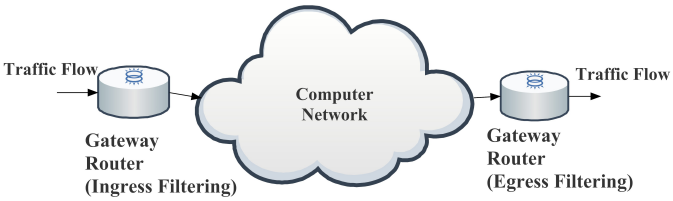

Fig. 9: Ingress/Egress Filtering

[31] A. Singh and B. B. Gupta, "Distributed denial-of-service (ddos) attacks and defense mechanisms in various web-enabled computing platforms: Issues, challenges, and future research directions," *International Journal on Semantic Web and Information Systems (IJSWIS)*, vol. 18, no. 1, pp. 1–43, 2022.

[32] E. Alomari, S. Manickam, B. Gupta, M. Anbar, R. M. Saad, and S. Alsaleem, "A survey of botnet-based ddos flooding attacks of application layer: Detection and mitigation approaches," in *Handbook of research on modern cryptographic solutions for computer and cyber security*. IGI Global, 2016, pp. 52–79.

[33] S. M. Specht and R. B. Lee, "Distributed denial of service: Taxonomies of attacks, tools, and countermeasures." in *ISCA PDCS*, 2004, pp. 543–550.

[34] S. Kumar, "Smurf-based distributed denial of service (ddos) attack amplification in internet," in *Internet Monitoring and Protection, 2007. ICIMP 2007. Second International Conference on*. IEEE, 2007, pp. 25–25.

[35] M. Bogdanoski, T. Shuminoski, and A. Risteski, "Analysis of the syn flood dos attack," *International Journal of Computer Network and Information Security*, vol. 5, no. 8, p. 1, 2013.

[36] M. Kenney. (1997) Ping of death. [Online]. Available: insecure.org/sploits/ping-o-death.html,

[37] C. C. Center, "Cert advisory ca-1997-28 ip denial-of-service attacks," 1997.

[38] S. Behal and K. Kumar, "Characterization and comparison of ddos attack tools and traffic generators: A review." *IJ Network Security*, vol. 19, no. 3, pp. 383–393, 2017.

[39] E. U. Opara and O. A. Soluade, "Straddling the next cyber frontier: The empirical analysis on network security, exploits, and vulnerabilities," *International Journal of Electronics and Information Engineering*, vol. 3, no. 1, pp. 10–18, 2015.

[40] D. Dittrich. (1999) The dos project's 'trinoo'distributed denial of service attack tool. [Online]. Available: staff.washington.edu/dittrich/misc/trinoo.analysis.txt

[41] A. Dahiya, B. B. Gupta, S. Yamaguchi, and K. Psannis, "Mitigating botnet based ddos attacks by selecting incentivized cooperating isps for risk transfer," in *2021 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2021, pp. 1–6.

[42] K. Alieyan, A. Almomani, M. Anbar, M. Alauthman, R. Abdullah, and B. B. Gupta, "Dns rule-based schema to botnet detection," *Enterprise Information Systems*, vol. 15, no. 4, pp. 545–564, 2021.

[43] P. J. Criscuolo, "Distributed denial of service: Trin00, tribe flood network, tribe flood network 2000, and stacheldraht ciac-2319," CALIFORNIA UNIV LIVERMORE RADIATION LAB, Tech. Rep., 2000.

[44] J. Barlow and W. Thrower, "Tfn2k–an analysis," *Axent Security Team*, 2000.

[45] D. Dittrich, "The 'stacheldraht'distributed denial of service attack tool," 1999. [Online]. Available: staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt

[46] D. Dittrich, G. Weaver, S. Dietrich, and N. Long, "The mstream distributed denial of service attack tool," *URL http://staff. washington. edu/dittrich/misc/mstream. analysis. txt*, vol. 3, 2000.

[47] B. Gupta, R. C. Joshi, and M. Misra, "Distributed denial of service prevention techniques," *arXiv preprint arXiv:1208.3557*, 2012.

[48] R. Singel. (2010) Operation payback cripples mastercard site in revenge for wikileaks ban. [Online]. Available: www.wired.com/threatlevel/2010/12/web20-attack-anonymous

[49] A. Dahiya and B. B. Gupta, "A reputation score policy and bayesian game theory based incentivized mechanism for ddos attacks mitigation and cyber defense," *Future Generation Computer Systems*, vol. 117, pp. 193–204, 2021.

[50] I. Cvitić, D. Peraković, B. Gupta, and K.-K. R. Choo, "Boosting-based ddos detection in internet of things systems," *IEEE Internet of Things Journal*, 2021.

[51] A. Dahiya and B. B. Gupta, "A qos ensuring two-layered multi-attribute auction mechanism to mitigate ddos attack," *Mobile Networks and Applications*, vol. 26, no. 3, pp. 1043–1058, 2021.

[52] R. Mehla, *Application of Deep Learning in Big Data Analytics for Healthcare Systems*. insights2techinfo.com, 2021. [Online]. Available: https://insights2techinfo.com/application-of-deep-learning-in-big-data-analytics-for-healthcare-systems/

[53] A. Khan and F. Penalvo, *Blockchain Technology and Associated Challenges in Smart Healthcare Systems*. insights2techinfo.com, 2021. [Online]. Available: https://insights2techinfo.com/blockchain-technology-and-associated-challenges-in-smart-healthcare-systems/

[54] D. Signla and S. Kr, *Blockchain for Data Science*. insights2techinfo.com, 2021. [Online]. Available: https://insights2techinfo.com/blockchain-for-data-science/

[55] B. Gupta and S. Harish, "Conceptual framework to mitigate internet of things-ddos attacks using fog nodes," *Recent Patents on Engineering*, vol. 15, no. 4, pp. 67–73, 2021.

[56] S. Kumar, *Artificial Intelligence and Machine learning for Smart and Secure Healthcare System*. Insights2Techinfo, 2021.

[57] K. Yadav, M. Quamara, and B. Gupta, *Hot Topics in Machine Learning Research*. Insights2Techinfo, 2021.

[58] U. Yadav, *AI Techniques in Information Management*. insights2techinfo.com, 2021. [Online]. Available: https://insights2techinfo.com/ai-techniques-in-information-management/

[59] Z. Zhou, A. Gaurav, B. B. Gupta, M. D. Lytras, and I. Razzak, "A fine-grained access control and security approach for intelligent vehicular transport in 6g communication system," *IEEE transactions on intelligent transportation systems*, 2021.

[60] A. Gaurav, B. B. Gupta, C.-H. Hsu, S. Yamaguchi, and K. T. Chui, "Fog layer-based ddos attack detection approach for internet-of-things (iots) devices," in *2021 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2021, pp. 1–5.

[61] A. Mishra, B. B. Gupta, D. Peraković, F. J. G. Peñalvo, and C.-H. Hsu, "Classification based machine learning for detection of ddos attack in cloud computing," in *2021 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2021, pp. 1–4.

[62] A. Gaurav and A. K. Singh, "Super-router: A collaborative filtering technique against ddos attacks," in *International Conference on Advanced Informatics for Computing Research*. Springer, 2017, pp. 294–305.

[63] D. K. Yau, J. Lui, F. Liang, and Y. Yam, "Defending against distributed denial-of-service attacks with max-min fair server-centric router throttles," *IEEE/ACM Transactions on Networking (TON)*, vol. 13, no. 1, pp. 29–42, 2005.

[64] N. Weiler, "Honeypots for distributed denial-of-service attacks," in *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE International Workshops on*. IEEE, 2002, pp. 109–114.

[65] R. Oppliger, "Internet security: firewalls and beyond," *Communications of the ACM*, vol. 40, no. 5, pp. 92–102, 1997.

[66] X. Geng and A. B. Whinston, "Defeating distributed denial of service attacks," *IT Professional*, vol. 2, no. 4, pp. 36–42, 2000.

[67] A. D. Keromytis, V. Misra, and D. Rubenstein, "Sos: An architecture for mitigating ddos attacks," *IEEE Journal on selected areas in communications*, vol. 22, no. 1, pp. 176–188, 2004.

[68] C. Jin, H. Wang, and K. G. Shin, "Hop-count filtering: an effective defense against spoofed ddos traffic," in *Proceedings of the 10th ACM conference on Computer and communications security*. ACM, 2003, pp. 30–41.

[69] D. Senie and P. Ferguson, "Network ingress filtering: Defeating denial of service attacks which employ ip source address spoofing," *Network*, 1998.

[70] K. Kalkan and F. Alagöz, "A distributed filtering mechanism against ddos attacks: Scoreforcore," *Computer Networks*, vol. 108, pp. 199–209, 2016.